WORKSHEET #6 – MATH 5405
SPRING 2016

NOT DUE

Let's review before the midterm. We start with short answer questions (just like on the midterm).

(1) Give an example of a ring R and elements $a, b \in R$ such that $a \neq 0 \neq b$ but $ab = 0$.

(2) Is $(\mathbb{Z}/2)[x]$ a field?

(3) Is $(\mathbb{Z}/2)[x]/(x^2 + x + 1)$ a field?

(4) Suppose I tell you that $x^4 + x^3 - x + 1$ is irreducible in $(\mathbb{Z}/5)[x]$. How many elements does the field $(\mathbb{Z}/5)[x]/(x^4 + x^3 - x + 1)$ have?

(5) What is the multiplicative inverse of x in $(\mathbb{Z}/3)/(x^2 + 1)$?

(6) Suppose you are trying to crack a Vigenére cipher using only the cipher text and you are given the following data from shifted incidence count / autocorrelation. When the text is shifted by the first row, there are the second row number of repeats. How long do you think the Vigenére key was?

1	2	3	4	5	6	7	8	9	10
43	52	47	76	61	44	47	80	49	50

(7) What are all the possible orders for an element of $(\mathbb{Z}/26)^\times$?

(8) Find a generator / primitive root for $(\mathbb{Z}/10)^\times$.

(9) Suppose Alice and Bob are using Diffie-Hellman to find a common key. Suppose that the common prime is $p = 28973513$ and a generator g is chosen. Suppose Alice chooses her secret key a and shares her part of the key $g^a \bmod p = 6743283$. If Bob chooses his secret key to be $b = 8923780$, what should Bob compute to find a common key. (Write out something that a computer could calculate, do not work it out).

(10) State what conditions on an integer $1 < a < n$ are needed to use the Rabin-Miller test to show that n is not prime (say $n - 1 = 2^k \cdot q$).

(11) What is a Carmichael number?

Let's now do some computations with classical ciphers.

(12) I encrypted the following phrase just like Caesar would have, by shifting all letters to the right by 3. Decrypt it.

`KHOORZRUOG`

(13) Encrypt the phrase `meowmeowmeow` using the Vigenére cipher and the keyword `CAT`.

(14) The following was encrypted using columnar transposition and the keyword `TANKS`. What was the original phrase? `HOGFTDTAEVHORLOADTATTEBTENAEIOBOIRSBINNFUOLSW`

Hint: It is a quote due to Churchill.

Let's do some computations with polynomials with coefficients from $\mathbb{Z}/p$. (15) Find the inverse of x^2 in $(\mathbb{Z}/3)[x]/(x^3 - x + 1)$.

(16) Find the multiplicative order of x in $(\mathbb{Z}/3)/(x^3 - x + 1)$.

This is probably slightly harder than I would put on an exam, but it's good practice. Do it in a smart way...

(17) Find all the elements of $(\mathbb{Z}/2[x])/(x^2 + x + 1)$ which are primitive roots / generators.

(18) Alice is setting up an RSA encryption system. She chooses two primes $p = 3, q = 5$ so that $m = pq = 15$ and chooses $e = 3$.

(a) Compute d, the multiplicative inverse of e mod $\varphi(m)$.

(b) After publishing the numbers (m, e), Bob sends Alice the encrypted message 8. What number did Bob encrypt?

(19) Suppose Alice is setting up an ElGamal encryption system.

(a) She picks her prime $p = 5$ and generator $g = 2$. She publishes $(p, g, g^a = 3)$. Take the role of Eve and figure out what a is.

(b) Suppose Bob picks his own secret number b and sends Alice $(2 = g^b, 1 = c)$. If Bob is using ElGamal, what was the message he was sending to Alice?